TRUST

E-Mails signieren und verschlüsseln

Benutzerhandbuch zur Signatur und Verschlüsselung
von E-Mails in Microsoft Outlook 2007

S-TRUST – ZERTIFIZIERUNGSDIENSTLEISTUNGEN DES DEUTSCHEN SPARKASSENVERLAGES

Inhalt

1. Wichtige Grundlagen **3**
1.1 Systemvoraussetzungen 4
1.2 E-Mails signieren und verschlüsseln 6
1.3 Wiederkehrende Arbeitsabläufe 9
1.4 Tipps zum Testen 12

2. Für Anwender von Microsoft Outlook 2007 **13**
2.1 Vorbereitende Grundeinstellungen 14
2.2 Schreiben signierter und verschlüsselter E-Mails 19
2.3 Lesen signierter und verschlüsselter E-Mails 21

3. Hinweise für Anwender anderer E-Mail-Programme **28**

4. Glossar **29**

5. Index **32**

1. Wichtige Grundlagen

Welche Kapitel sollten Sie lesen?
In diesem Benutzerhandbuch wird erläutert, wie Sie E-Mails mit S-TRUST Personenzertifikaten signieren, verschlüsseln und entschlüsseln.

Relevant sind für Sie zwei Kapitel:
- „Wichtige Grundlagen“ sowie
- das Kapitel „Für Anwender von Microsoft Outlook 2007“

Falls Sie ein E-Mail-Programm nutzen, das in diesem Handbuch nicht aufgeführt ist, beachten Sie bitte die Abschnitte „Systemvoraussetzungen“ auf Seite 4 sowie das Kapitel 3 „Hinweise für Anwender anderer E-Mail-Programme“ ab Seite 28.

Im Glossar ab Seite 31 werden einige Fachbegriffe erklärt.

Ergänzende Hintergrundinformationen
Allgemeine Informationen zum Thema digitale Signatur und deren rechtlicher Bedeutung finden Sie auf der Internetseite *www.s-trust.de*.

Eine umfangreiche Einführung in die technischen Grundlagen der digitalen Signatur und Verschlüsselung gibt das elektronische Handbuch von S-TRUST Sign-it, das unter *www.s-trust.de/produkte_leistungen/signatursoftware/software_einzelsignatur/index.htm* heruntergeladen werden kann.

FAQ – Häufig gestellte Fragen
Aktuelle Antworten zu häufig gestellten Fragen (FAQ) können Sie im Internet unter folgender Adresse abrufen: *www.openlimit.com/faq*.

Hotline
Technische Fragen zur Nutzung Ihres E-Mail-Programms in Verbindung mit S-TRUST Sign-it beantwortet eine technische Supporthotline montags bis sonntags von 8 bis 22 Uhr unter 0900 1 47 88 77 (1,99 €/Min. aus dem Festnetz der Deutschen Telekom).

1.1 Systemvoraussetzungen

Software von CD-ROM
Alle Erläuterungen in diesem Handbuch setzen voraus, dass die Software von der CD-ROM „Qualifizierte Signatur von S-TRUST“ bereits installiert wurde.

S-TRUST Sign-it
Zusätzlich benötigen Sie die Software S-TRUST Sign-it (Vollversion oder eine noch nicht abgelaufene 30-Tage-Testlizenz). Ist die 30-Tage-Testlizenz abgelaufen, kann bei Kauf einer Softwarelizenz *(unter www.sparkassen-shop.de)* das Produkt weiter genutzt werden. Eine Anleitung zur Freischaltung der Lizenz finden Sie in der Dokumentation „S-TRUST Sign-it Elektronisches Handbuch“.

Hinweis:
Falls Sie mehrere Zertifikate nutzen, muss in S-TRUST Sign-it unter *Einstellungen > Zertifikate* die Option *Automatisch registrierte Zertifikate ständig verfügbar halten* aktiviert sein.

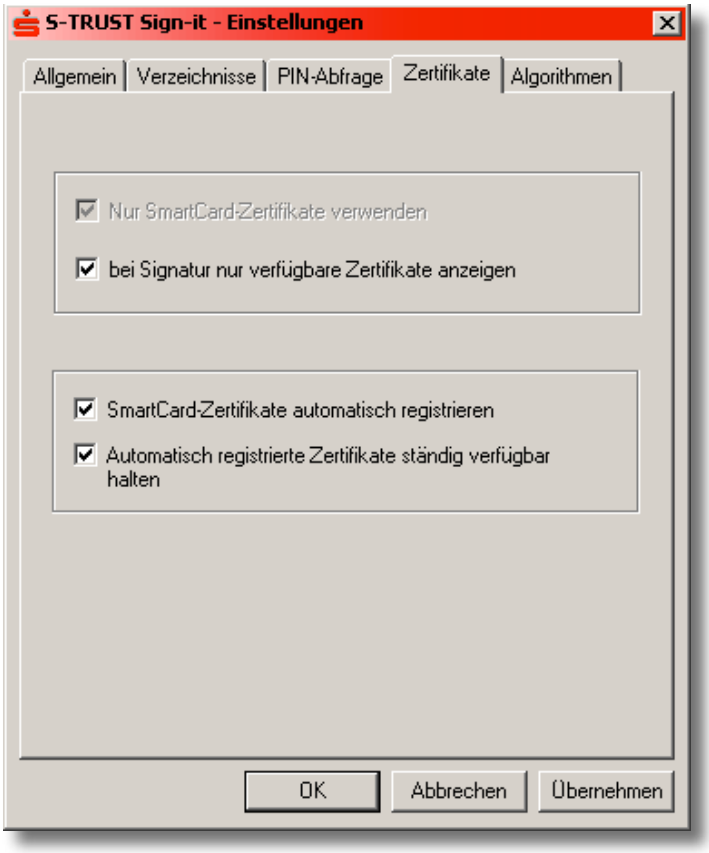

Abbildung 1.1: Software S-TRUST Sign-it – Einstellungen > Zertifikate

Service Packs und Updates
Wir empfehlen, alle Service Packs und Updates von Microsoft zu installieren.

Kartenleser und Karte
Ihr Kartenleser muss an Ihren Computer angeschlossen sein und Ihre signaturfähige Karte der Sparkassen-Finanzgruppe muss sich im Kartenleser befinden.

Unterstützte E-Mail-Programme
Um E-Mails signieren und verschlüsseln zu können, benötigen Sie ein E-Mail-Programm, das diese Funktionen unterstützt. Die folgenden Beschreibungen gehen davon aus, dass ein solches E-Mail-Programm bereits installiert und eingerichtet wurde.

Hinweis:
Die E-Mail-Adresse, von der Sie signierte und verschlüsselte E-Mails verschicken, muss die identische E-Mail-Adresse sein, für welche die Zertifikate auf Ihrer Karte ausgestellt wurden.

Folgende E-Mail-Programme wurden vom Deutschen Sparkassenverlag getestet und für die Verwendung mit S-TRUST Personenzertifikaten freigegeben:

- Microsoft Outlook Express
- Windows Live Mail
- Microsoft Outlook 2000
- Microsoft Outlook 2003
- Microsoft Outlook 2007[1]
- Mozilla Thunderbird

Wenn Sie ein anderes E-Mail-Programm oder eine andere Version eines der genannten Programme einsetzen möchten, übernimmt der Deutsche Sparkassenverlag hierfür keine Gewähr. In diesem Fall kann die Vorgehensweise von den in den jeweiligen Benutzerhandbüchern gezeigten Schritten und Abbildungen abweichen. Bitte beachten Sie dazu auch die Informationen im Kapitel „Hinweise für Anwender anderer E-Mail-Programme“ ab Seite 28.

[1] *Outlook 2007 wird zurzeit aufgrund von Fehlern seitens Microsoft von S-Trust Sign-it nicht vollständig unterstützt. Details dazu finden Sie auf Seite 13.*

1.2 E-Mails signieren und verschlüsseln

Was passiert eigentlich, wenn eine E-Mail signiert oder verschlüsselt wird? Das Grundwissen über die elementaren Abläufe beim Signieren und Verschlüsseln erleichtert Ihnen das Verständnis für die erforderlichen Arbeitsschritte.

Privater Schlüssel und öffentlicher Schlüssel
Für die Signatur und Verschlüsselung von E-Mails benötigen Sie zwei Schlüssel: den privaten Schlüssel und den öffentlichen Schlüssel. Diese Schlüssel ergänzen sich gegenseitig. Daten, die mit dem einen Schlüssel verschlüsselt wurden, können grundsätzlich nur mit dem anderen Schlüssel wieder entschlüsselt werden.
Ihr *privater Schlüssel* befindet sich auf dem Chip Ihrer signaturfähigen Karte der Sparkassen-Finanzgruppe. Aus Sicherheitsgründen lässt er sich nicht auslesen und wird auch nicht an Ihren Computer übertragen. Mit dem privaten Schlüssel wird eine E-Mail signiert und eine verschlüsselte E-Mail entschlüsselt.
Ihr *öffentlicher Schlüssel* ist in Ihr Zertifikat integriert und z. B. in Verzeichnisdiensten im Internet frei abrufbar. Mit dem öffentlichen Schlüssel werden E-Mails verschlüsselt. Der verschlüsselte Text kann nur mit dem privaten Schlüssel des Empfängers wieder entschlüsselt werden. Auch wenn Sie eine signierte, aber nicht verschlüsselte E-Mail versenden, erhält der Empfänger Ihren öffentlichen Schlüssel. Um sicherzugehen, dass das Zertifikat und somit auch der Schlüssel nicht gefälscht wurden, sollten folgende Punkte geprüft werden:

- Ist das Dokument unverändert?
- Authentizität des Zertifikatsinhabers?
- Ist das Zertifikat gesperrt?

Einige Punkte prüft die Software automatisch. Es liegt jedoch in der Entscheidung des Benutzers, ob er einem Zertifikat vertraut. Qualifizierte Signaturen nach dem deutschen Signaturgesetz lassen sich lückenlos zurückverfolgen bis zur Bundesnetzagentur, das Herausgeberzertifikat der Bundesnetzagentur ist in die Software integriert. Dieser Zertifizierungspfad muss mathematisch korrekt und lückenlos sein. Aber auch andere Wurzelzertifikate können vom Nutzer im Betriebssystem als vertrauenswürdig definiert werden.

Was passiert beim Signieren?
Damit elektronische Kommunikation sicher erfolgen kann, muss die E-Mail mit einer digitalen Signatur versehen sein, vergleichbar mit einer Unterschrift. Diese Signatur wird mit Ihrem *privaten Schlüssel* erstellt. So kann der Empfänger sicher sein, dass die E-Mail tatsächlich von Ihnen stammt, denn nur Sie verfügen über den privaten Schlüssel auf Ihrer Karte und die dazugehörige PIN. Es erfolgt eine Prüfung der Signatur mit dem *öffentlichen Schlüssel* um sicherzugehen, dass die Signatur nicht gefälscht wurde, der Zertifikatsinhaber also echt ist. Dabei werden außer dem Namen und der E-Mail-Adresse keine persönlichen Daten des Inhabers preisgegeben.

Als weitere Sicherheitsstufe wird beim Signieren der E-Mail eine Prüfsumme gebildet. Wird die E-Mail bei der Übertragung vorsätzlich oder unbeabsichtigt verändert, stimmt diese Prüfsumme nicht mehr, erhält der Empfänger eine Warnung, dass die E-Mail verändert wurde und die Signatur damit ungültig ist.

Was passiert beim Verschlüsseln?
Die Verschlüsselung verwendet die beiden Schlüssel in umgekehrter Reihenfolge. Eine E-Mail wird zunächst mit dem *öffentlichen Schlüssel* des Empfängers verschlüsselt. Nur er kann die Nachricht mit seinem *privaten Schlüssel* wieder entschlüsseln.

ACHTUNG:
Da zum Verschlüsseln ausschließlich der öffentliche Schlüssel des Empfängers verwendet wird, kann auch nur der Empfänger die Nachricht mit dem zugehörigen privaten Schlüssel wieder entschlüsseln. Dies bedeutet: Auch Sie als Absender können die verschlüsselte E-Mail nicht mehr lesen! Die Kopie im Ordner „Gesendete Objekte" kann NICHT geöffnet werden!
Deshalb sollten Sie die verschlüsselte E-Mail auch an sich selbst unter „CC" oder „BCC" schicken. Dann erhalten Sie je nach Einstellung in Ihrem E-Mail-Programm entweder ein unverschlüsseltes Duplikat oder ein mit Ihrem eigenen öffentlichen Schlüssel verschlüsseltes Duplikat, das Sie selbst wieder öffnen können.

So erhalten Sie das Zertifikat eines Empfängers

Per E-Mail
Um eine verschlüsselte E-Mail an eine andere Person zu versenden, benötigen Sie den öffentlichen Schlüssel des Empfängers. Dazu muss er Ihnen eine signierte E-Mail schicken. Am besten speichern Sie seine E-Mail-Adresse sowie das Zertifikat in Ihrem Adressbuch.

Verzeichnisdienst
Sie haben aber auch die Möglichkeit, Zertifikate aus einem Verzeichnisdienst herunterzuladen.
Auf *www.zvs-user.s-trust.de* können Sie S-TRUST-Zertifikate anderer Personen suchen und herunterladen.

Unter dem Menüpunkt *Suchen von Zertifikaten* wird Ihnen eine Suchmaske zur Suche von Zertifikaten angezeigt. Alternativ können Sie auch über *www.s-trust.de* unter der Rubrik Zertifikatsmanagement dem Link *Download qualifizierter Zertifikate* und dann *Downloadserver von S-TRUST* folgen.

Abbildung 1.2: Suchen von Personenzertifikaten unter www.zvs-user.s-trust.de

Weitere Informationen zum Thema Herunterladen von Zertifikaten finden Sie auf der CD-ROM „Qualifizierte Signatur von S-TRUST“ im Dokument „Gebrauchsanleitung für qualifizierte S-TRUST Personenzertifikate“.

Gültigkeit eines Zertifikats
Zertifikate werden bei Diebstahl oder Verlust der Karte gesperrt. Verschiedene Institutionen (u.a. Bundesnetzagentur, S-TRUST) verwalten Sperrlisten, in denen ungültige Zertifikate aufgeführt sind. Um sicherzugehen, dass bei der Zertifikatsprüfung kein gesperrtes Zertifikat akzeptiert wird, müssen Sie Ihre Einstellungen regelmäßig aktualisieren. Dazu rufen Sie in der Software S-TRUST Sign-it die Funktion „Sperrlistenaktualisierung“ auf. Eine Beschreibung der Funktion finden Sie im elektronischen Benutzerhandbuch von S-TRUST Sign-it.

ACHTUNG:
Sperrlisten werden von den verschiedenen E-Mail-Programmen nicht einheitlich verwendet. Es kann also sein, das die in Ihrem E-Mail-Programm angezeigte Gültigkeit eines Zertifikats nicht zuverlässig ist. Wir empfehlen daher, für die Überprüfung der Gültigkeit eines Zertifikats ausschließlich die Signatursoftware S-TRUST Sign-it zu verwenden.

Eine ausführliche Beschreibung zur Prüfung der Gültigkeit eines Zertifikats finden Sie im Kapitel „Arbeitsabläufe“ im Elektronischen Benutzerhandbuch von S-TRUST Sign-it.

Bindung an eine E-Mail-Adresse
Das Verschlüsselungszertifikat ist einer bestimmten E-Mail-Adresse zugeordnet. Falls der Empfänger Ihrer verschlüsselten E-Mail unter mehreren E-Mail-Adressen erreichbar ist, müssen Sie Ihre verschlüsselte Nachricht an die E-Mail-Adresse senden, für die das Zertifikat ausgestellt wurde.

ZUSAMMENFASSUNG

Wenn Sie …	benötigen Sie …	Erklärung
… eine signierte E-Mail senden	… Ihre CSA-PIN.	Ihre Signatur wird auf Ihrer Karte erzeugt.
… eine signierte E-Mail empfangen	… nichts.	Den öffentlichen Schlüssel erhalten Sie vom Absender zusammen mit der E-Mail.
… eine verschlüsselte E-Mail senden	… den öffentlichen Schlüssel des Empfängers. [2]	Die E-Mail wird ausschließlich mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und kann nur vom Empfänger mit seinem privaten Schlüssel wieder entschlüsselt werden.
… eine verschlüsselte E-Mail empfangen	… Ihre CSA-PIN.	Die E-Mail wird mit dem privaten Schlüssel auf Ihrer Karte wieder entschlüsselt.

[2] *Den öffentlichen Schlüssel erhalten Sie entweder über einen Verzeichnisdienst im Internet oder aber zusammen mit einer signierten E-Mail, die Ihnen der Empfänger zuvor geschickt hat. Falls Sie eine lesbare Kopie der E-Mail aufbewahren wollen, müssen Sie diese als „CC“ oder „BCC“ an Ihre eigene E-Mail-Adresse schicken.*

1.3 Wiederkehrende Arbeitsabläufe

Signatur erzeugen
Jedes Mal, wenn Sie eine E-Mail signieren möchten, werden Sie von S-TRUST Sign-it aufgefordert, eine Signatur zu erzeugen. Die Vorgehensweise dabei ist unabhängig davon, welches E-Mail-Programm Sie verwenden.

Beim Absenden der E-Mail erscheint automatisch das Fenster *S-TRUST Sign-it Signaturanforderung:*

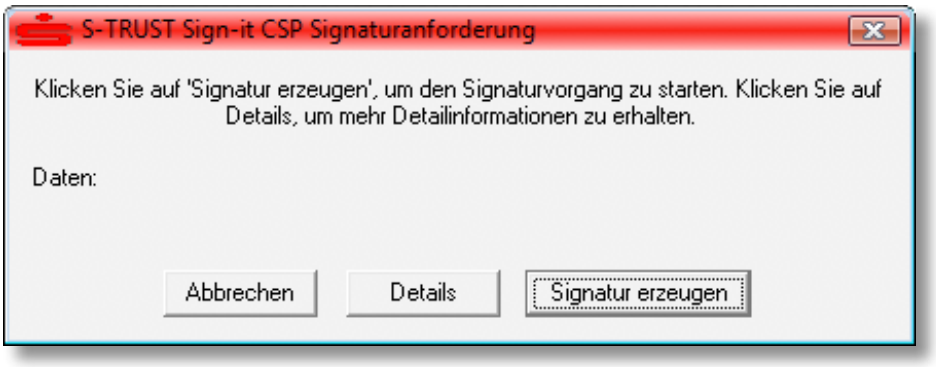
S-TRUST Sign-it CSP Signaturanforderung
Klicken Sie auf 'Signatur erzeugen', um den Signaturvorgang zu starten. Klicken Sie auf Details, um mehr Detailinformationen zu erhalten.
Daten:
Abbrechen
Details
Signatur erzeugen

Abbildung 1.3: S-TRUST Sign-it Signaturanforderung

1. Betätigen Sie die Schaltfläche *Signatur erzeugen*.
   Je nachdem welches Kartenlesegerät Sie verwenden, erscheint ein Sicherheitshinweis zur PIN-Eingabe.

S-TRUST Sign-it
Wir empfehlen, die Eingabe der PIN (CSA-Passwort) nur auf einem Kartenleser mit sicherer PIN-Eingabe durchzuführen!
OK

Abbildung 1.4: Warnmeldung zur sicheren PIN-Eingabe am Kartenlesegerät

2. Bestätigen Sie mit *OK*.
Sie werden nun aufgefordert, Ihre CSA-PIN einzugeben.

CSA-PIN eingeben
Ihre CSA-PIN müssen Sie jedes Mal eingeben, wenn Sie
- eine Signatur erzeugen, also eine E-Mail signieren oder
- eine für Sie verschlüsselte Nachricht entschlüsseln.

Die Vorgehensweise ist dabei identisch und unabhängig davon, welches E-Mail-Programm Sie verwenden. Es erscheint automatisch das Fenster S-TRUST Sign-it oder Sie werden direkt am Kartenleser aufgefordert Ihre CSA-PIN einzugeben.

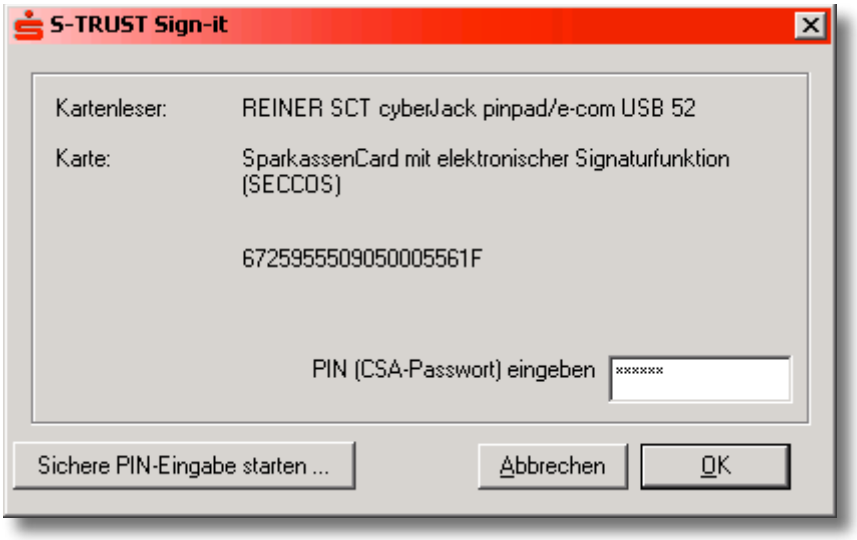

Abbildung 1.5: CSA-PIN-Eingabe

ACHTUNG:
Aus Sicherheitsgründen sollten Sie Ihre CSA-PIN grundsätzlich immer direkt am Kartenleser und nicht über die Tastatur Ihres Computers eingeben. Eine Eingabe direkt am Kartenlesegerät ist jedoch nur möglich, wenn Ihre CSA-PIN ausschließlich aus Ziffern und nicht aus Buchstaben besteht.

So geben Sie die CSA-PIN direkt am Kartenleser ein (Abbildung 1.6):

1. Klicken Sie auf die Schaltfläche *Sichere PIN-Eingabe* starten. Sie werden nun aufgefordert, Ihre CSA-PIN direkt am Kartenleser einzugeben.

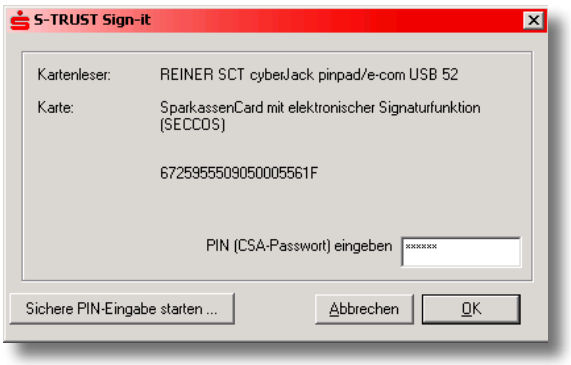

Abbildung 1.6: Sichere CSA-PIN-Eingabe am Kartenleser

2. Geben Sie jetzt direkt am Kartenleser die CSA-PIN Ihrer Karte ein.

3. Bestätigen Sie Ihre Eingabe durch Drücken der grünen OK-Taste direkt am Kartenleser.

Über die Tastatur Ihres Computers können Sie Ihre CSA-PIN ebenfalls eingeben (Abbildung 1.5):

1. Geben Sie im Fenster *S-TRUST Sign-it* die CSA-PIN Ihrer Karte in das Eingabefeld ein.

2. Bestätigen Sie mit *OK*.
   In beiden Fällen der PIN-Eingabe führt Ihr E-Mail-Programm die begonnene Aktion (Signieren oder Entschlüsseln) nun aus.

HINWEIS:
Unterläuft Ihnen bei der Eingabe der CSA-PIN ein Fehler, haben Sie noch zwei weitere Versuche, die korrekte PIN einzugeben. Nach drei Fehleingaben wird die CSA-PIN auf Ihrer Karte gesperrt. In diesem Falle müssen Sie die PIN wieder entsperren. Informationen dazu finden Sie in der „Gebrauchsanleitung für qualifizierte S-TRUST Personenzertifikate", die Sie unter *www.s-trust.de* herunterladen können.

1.4 Tipps zum Testen

Um mit dem Schreiben und Lesen signierter und verschlüsselter E-Mails schnell und sicher vertraut zu werden, sollten Sie die Beschreibungen dieses Handbuchs möglichst selbst auf Ihrem Computer nachvollziehen.

Falls Sie keinen E-Mail-Partner haben, mit dem Sie zum Test signierte und verschlüsselte E-Mails austauschen können, empfehlen wir Ihnen folgendes Vorgehen:

1. Nehmen Sie wie für Ihr E-Mail-Programm beschrieben die erforderlichen Grundeinstellungen vor.
2. Schreiben Sie an Ihre eigene E-Mail-Adresse eine signierte, aber nicht verschlüsselte Nachricht.
3. Rufen Sie diese Nachricht ab und nehmen Sie Ihre eigene E-Mail-Adresse und damit Ihr Zertifikat wie beschrieben in das Adressbuch Ihres E-Mail-Programms auf.

Nun können Sie sich selbst beliebige signierte und verschlüsselte E-Mails schicken und alle Funktionen ausführlich und sicher testen.

Eine detaillierte Anleitung zum Versand von signierten und verschlüsselten E-Mails über Ihr E-Mail-Programm finden Sie in den jeweiligen Benutzerhandbüchern.

2 Microsoft Outlook 2007

In diesem Kapitel wird erklärt, wie die Signatur und Verschlüsselung von E-Mails mit Microsoft Outlook 2007 funktioniert.

Die folgenden Abbildungen zeigen ausschließlich die Einrichtung und Verwendung von S-Trust Sign-it am Beispiel von Microsoft Outlook 2007. Falls Sie eine andere Version von Microsoft Outlook verwenden möchten, beachten Sie bitte die jeweiligen Benutzerhandbücher sowie die Informationen im Abschnitt „Systemvoraussetzungen“ auf Seite 4.

WICHTIGER HINWEIS

Outlook 2007 wird zurzeit aufgrund von Fehlern seitens Microsoft nicht vollständig unterstützt.
Es können folgende Fehler auftreten:

- **Keine Speicherung der ausgewählten Zertifikate zur Verschlüsselung und Signatur.**
- **Keine Überprüfung der Zertifikatssperrlisten. Outlook kann somit nicht überprüfen, ob das eingesetzte Zertifikat gesperrt ist.**
- **Keine Darstellung verschlüsselter Nachrichten im Vorschaufenster (Lesebereich).**

2.1 Vorbereitende Grundeinstellungen

Sicherheitseinstellungen vornehmen
Zunächst sind folgende Sicherheitseinstellungen in Outlook 2007 vorzunehmen:

1. Stecken Sie Ihre signaturfähige Karte der Sparkassen-Finanzgruppe mit elektronischer Signatur in den Kartenleser.

2. Wählen Sie in Outlook 2007 den Menüpunkt *Extras > Vertrauensstellencenter.* Es öffnet sich das Fenster Vertrauensstellencenter.

3. Aktivieren Sie die Registerkarte *E-Mail Sicherheit*.

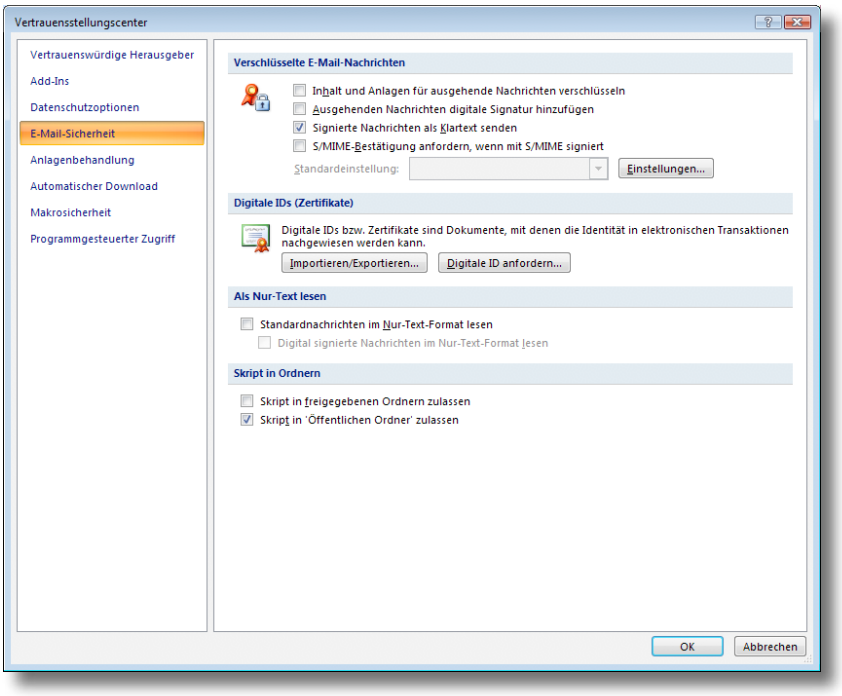

Abbildung 2.1: Outlook 2007 – Vertrauensstellencenter, Registerkarte E-Mail-Sicherheit

4. Klicken Sie im Feld *Verschlüsselte E-Mail-Nachrichten* auf die Schaltfläche *Einstellungen*. Es öffnet sich das Fenster Sicherheitseinstellungen ändern (Abb. 2.2).
Hinweis: Wenn sich stattdessen das Fenster E-Mail-Sicherheit öffnet, überprüfen Sie bitte, ob Ihr Kartenlesegerät korrekt installiert ist und sich Ihre Signaturkarte darin befindet.

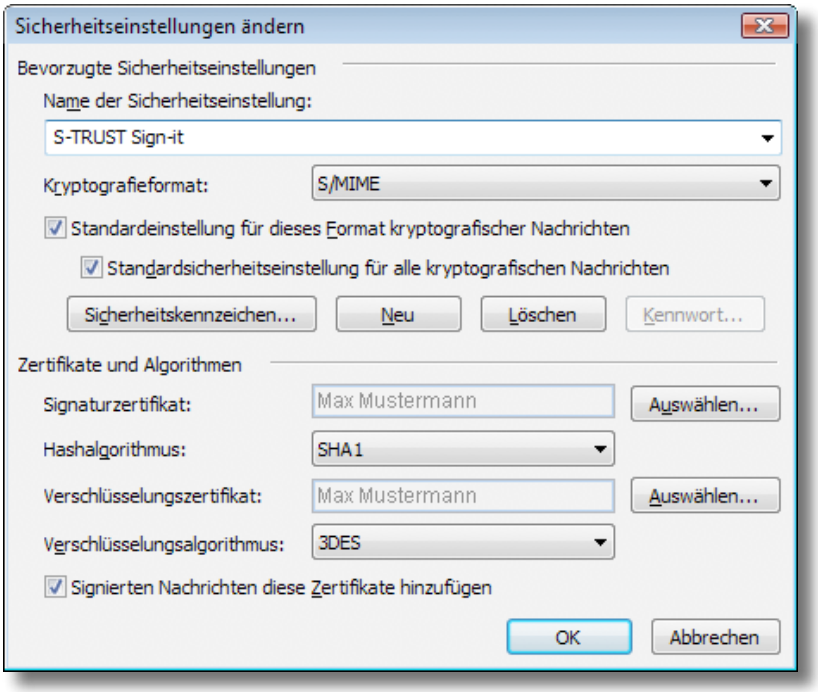

Abbildung 2.2: Outlook 2007 – Sicherheitseinstellungen ändern

- Geben Sie im Feld *Name der Sicherheitseinstellung* einen Namen für die Sicherheitseinstellung ein, zum Beispiel „S-TRUST Sign-it“.
- Wählen Sie als Kryptografieformat die Option *S/MIME*.
- Aktivieren Sie die Optionen *Standardeinstellung für dieses Format kryptografischer Nachrichten* und *Standardsicherheitseinstellung für alle kryptografischen Nachrichten* sowie im unteren Bereich von Zertifikate und Algorithmen die Option *Signierten Nachrichten diese Zertifikate hinzufügen* – wenn diese nicht bereits ausgewählt sind.
- Im Anschluss bestimmen Sie Ihre Zertifikate (siehe unten) und wählen im Bereich Zertifikate und Algorithmen für *Hashalgorithmus* die Option *SHA1* und für *Verschlüsselungsalgorithmus* die Option *3DES*.

Zertifikate auswählen
Jetzt wählen Sie das Signaturzertifikat und das Verschlüsselungszertifikat, das Sie beim Versenden von E-Mails nutzen möchten.
Zunächst wird das Zertifikat für den Signiervorgang (Signaturzertifikat) bestimmt.

1. Klicken Sie im bereits geöffneten Fenster *Sicherheitseinstellungen ändern* (siehe oben) unter *Zertifikate und Algorithmen* in der Zeile *Signaturzertifikat* auf die Schaltfläche *Auswählen*. Es öffnet sich ein Fenster, in dem die auf Ihrem System zur Verfügung stehenden Zertifikate aufgeführt sind.

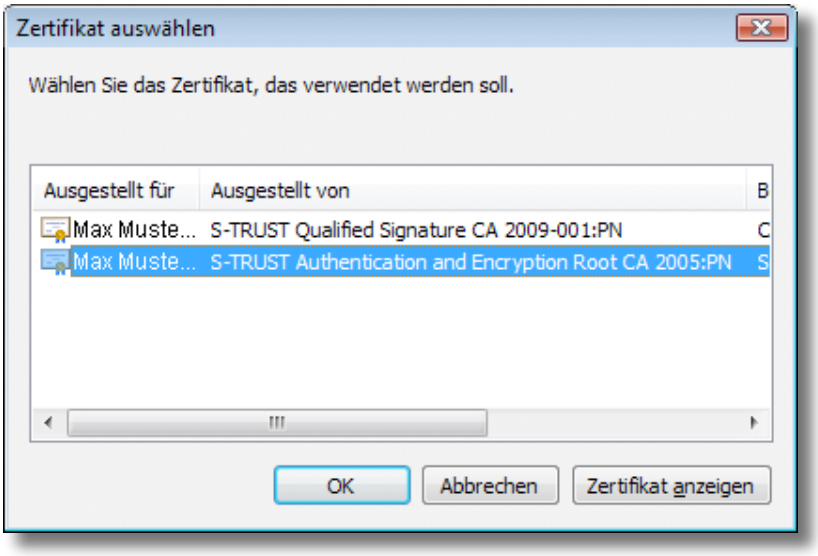

Abbildung 2.3: Outlook 2007 – Zertifikat auswählen

2. Markieren Sie in der Spalte *Ausgestellt von* das Zertifikat mit dem Eintrag *S-TRUST Authentication and Encryption Root CA 200x:PN*. Hinweis: Sind die Einträge abgeschnitten bzw. mit „…“ versehen, können Sie die Spalten mit der Maus wie in Listen üblich vergrößern.

3. Bestätigen Sie mit *OK*. Sie befinden sich nun wieder im Fenster Sicherheitseinstellungen ändern. Das soeben ausgewählte Zertifikat erscheint nun mit Ihrem Namen grau hinterlegt für den Signiervorgang im Feld Signaturzertifikat (Abb. 2.2).

Im nächsten Schritt wählen Sie das Zertifikat für den Verschlüsselungsvorgang (Verschlüsselungszertifikat) aus. Standardmäßig wird hierzu dasselbe Zertifikat wie für den Signaturvorgang verwendet.
Sollten Sie stattdessen ein anderes Zertifikat nutzen wollen, nehmen Sie folgende Einstellungen vor:

1. Im Fenster *Sicherheitseinstellungen ändern* klicken Sie in der Zeile *Verschlüsselungszertifikat* auf die Schaltfläche *Auswählen*. Es öffnet sich erneut das Fenster, in dem die auf Ihrem System zur Verfügung stehenden Zertifikate aufgeführt sind.

2. Markieren Sie in der Spalte *Ausgestellt von* das Zertifikat mit dem Eintrag *S-TRUST Authentication and Encryption Root CA 200x:PN*.

3. Bestätigen Sie mit *OK*.
   Sie befinden sich nun wieder im Fenster Sicherheitseinstellungen ändern. Das soeben ausgewählte Zertifikat für den Verschlüsselungsvorgang erscheint nun mit Ihrem Namen grau hinterlegt im Feld Verschlüsselungszertifikat (Abb. 2.2).

4. Verlassen Sie das Fenster Sicherheitseinstellungen ändern mit *OK*. Sie befinden sich nun wieder im Fenster Vertrauensstellungscenter (Abb. 2.1).

Signieren und Verschlüsseln als Voreinstellung
Wenn Sie die meisten E-Mails signiert oder verschlüsselt versenden, können Sie dies in Outlook 2007 voreinstellen. Outlook 2007 signiert und verschlüsselt dann automatisch alle von Ihnen gesendeten E-Mails, sofern Sie diese Funktion nicht explizit für einzelne E-Mails ausschalten.
So stellen Sie die automatische Verschlüsselung aller E-Mails ein:

1. Öffnen Sie das Fenster Vertrauensstellungscenter über den Menüpunkt *Extras > Vertrauensstellungscenter* (Abb. 2.1).

2. Aktivieren Sie die Registerkarte *E-Mail-Sicherheit*.

3. Um alle ausgehenden E-Mails automatisch zu signieren, aktivieren Sie die Option *Ausgehenden Nachrichten digitale Signatur hinzufügen* (Abb. 2.1).

4. Um alle ausgehenden E-Mails automatisch zu verschlüsseln, wählen Sie die Option *Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln* (Abb. 2.1).

5. Bestätigen Sie mit *OK*.

Codierung einstellen
Je nach Codierungseinstellung kann es mit älteren E-Mail-Servern zu Problemen kommen. Deshalb sollten Sie die Codierung in Ihrem E-Mail-Programm auf Unicode (UTF-8) einstellen:

1. Öffnen Sie dazu das Fenster Optionen über den Menüpunkt *Extras > Optionen*.

2. Aktivieren Sie die Registerkarte *E-Mail-Format*.

3. Klicken Sie im Bereich *Nachrichtenformat* auf die Schaltfläche *Internationale Optionen*. Es öffnet sich das Fenster Internationale Optionen (Abb. 2.4).

4. Unter *Codierungsoptionen* wählen Sie unter *Bevorzugte Codierung für ausgehende Nachrichten* in der Auswahlliste die Option *Unicode* (UTF-8).

5. Schließen Sie alle noch offenen Fenster mit *OK*.

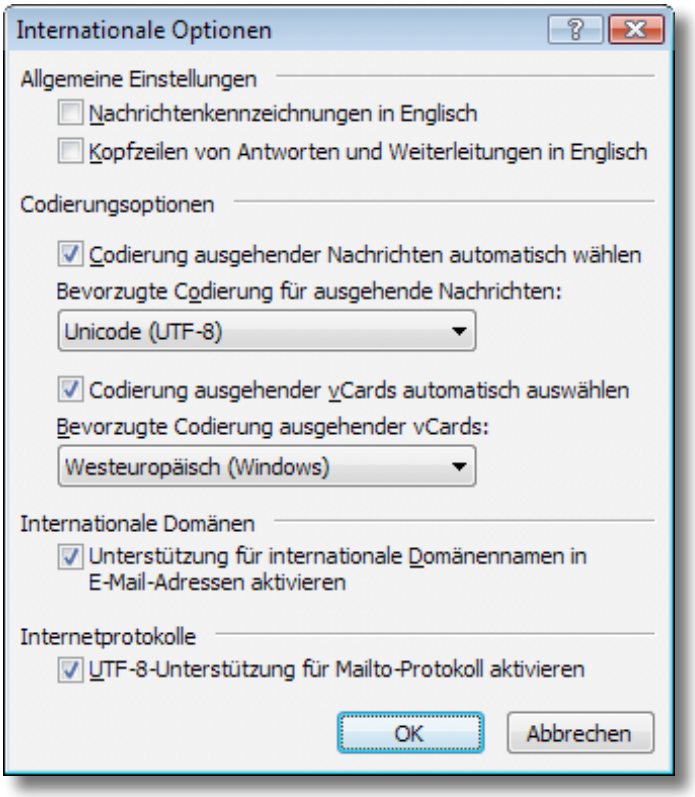

Abbildung 2.4: Outlook 2007 – Internationale Optionen

2.2 Schreiben signierter und verschlüsselter E-Mails

Ihre E-Mails können Sie signieren oder verschlüsseln sowie gleichzeitig signieren und verschlüsseln. Das Vorgehen ist in allen Fällen nahezu identisch. Selbstverständlich können Sie einzelne E-Mails auch weiterhin unsigniert und unverschlüsselt verschicken. Um eine E-Mail zu signieren, benötigen Sie den privaten Schlüssel auf Ihrer Signaturkarte. Für die Verschlüsselung einer E-Mail benötigen Sie den öffentlichen Schlüssel aus dem Zertifikat des Empfängers.

ACHTUNG:
Nur der Empfänger kann die für ihn verschlüsselte Nachricht wieder entschlüsseln, da nur er den dafür erforderlichen privaten Schlüssel besitzt. Auch Sie als Absender können die E-Mail nicht mehr entschlüsseln! Beachten Sie hierzu bitte auch die Hinweise unter „Was passiert beim Verschlüsseln?“ auf Seite 6.

Integration des öffentlichen Schlüssels eines Empfängers

Fall 1:
Der Empfänger Ihrer verschlüsselten Nachricht hat Ihnen bereits eine signierte E-Mail zugeschickt. Sie haben sein Zertifikat daraufhin wie im Abschnitt „Zertifikat des Absenders zum Adressbuch hinzufügen“ auf Seite 25 beschrieben zum Adressbuch von Outlook 2007 hinzugefügt.

Fall 2:
Der Empfänger Ihrer verschlüsselten Nachricht hat Ihnen sein Verschlüsselungszertifikat als E-Mail-Anhang geschickt oder Sie haben das Zertifikat aus einem Verzeichnisdienst heruntergeladen (siehe „So erhalten Sie das Zertifikat eines Empfängers“ auf Seite 7):

1. Speichern Sie die Datei mit dem Verschlüsselungszertifikat auf Ihrem Computer.
2. Legen Sie im Adressbuch von Outlook 2007 einen neuen Eintrag an oder öffnen Sie den Adressbucheintrag, falls dieser bereits existiert. Sie befinden sich nun im Fenster mit den Angaben zu Ihrem Kontakt (vgl. Abb. 2.9).
3. Aktivieren Sie in der Symbolleiste unter *Anzeigen* die Registerkarte *Zertifikate*.
4. Klicken Sie auf die Schaltfläche *Importieren* und wählen Sie die Zertifikatsdatei Ihres Kontaktes aus, die Sie zuvor auf Ihrem Computer gespeichert haben. Das Zertifikat erscheint nun in der Liste.
5. Klicken Sie in der Symbolleiste unter *Aktionen* auf die Schaltfläche *Speichern & schließen*.

E-Mail signieren und verschlüsseln
Eine E-Mail wird in folgenden Schritten signiert und verschlüsselt.

1. Schreiben Sie Ihre E-Mail und fügen Sie wie gewohnt Dateien als Anhang an.

2. Klicken Sie in der Symbolleiste des E-Mail-Fensters auf die Symbole für die Signatur bzw. Verschlüsselung einer E-Mail oder auf beide:

E-Mail signieren Icon1

E-Mail verschlüsseln Icon2

3. Mit einem Klick auf die Schaltfläche *Senden* schicken Sie Ihre Nachricht wie gewohnt ab.

4. Wenn Sie zuvor die Option **E-Mail signieren** aktiviert haben, werden Sie nun von „S-TRUST Sign-it“ aufgefordert, eine Signatur zu erzeugen und die CSA-PIN Ihrer Karte einzugeben (siehe „Wiederkehrende Arbeitsabläufe“ auf Seite 9). Die E-Mail wird jetzt wie gewohnt versendet.

2.3 Lesen signierter und verschlüsselter E-Mails

Outlook 2007 zeigt durch folgende Symbole an, wenn eine eingehende E-Mail signiert oder verschlüsselt bzw. signiert und verschlüsselt ist:

signierte E-Mail

verschlüsselte E-Mail

Signierte und verschlüsselte E-Mails öffnen

So öffnen Sie eine signierte und verschlüsselte E-Mail:

1. Markieren oder doppelklicken Sie die E-Mail wie gewohnt im Vorschaufenster von Outlook.
   Hinweis: Durch einen Fehler in Outlook 2007 werden verschlüsselte E-Mails trotz korrekter Eingabe der PIN nicht im Vorschaufenster angezeigt, sondern es erscheint die Meldung „Diese verschlüsselte Nachricht kann im Lesebereich nicht angezeigt werden“.
   Empfehlung: Deaktivieren Sie das automatische Vorschaufenster. Wählen Sie dazu im Menü Ansicht den Punkt *Lesebereich > Aus*
2. Falls die E-Mail nur signiert, jedoch nicht verschlüsselt wurde, öffnet sie sich sofort. Wurde die E-Mail jedoch verschlüsselt bzw. signiert und verschlüsselt, werden Sie von S-TRUST Sign-it aufgefordert, die CSA-PIN Ihrer Karte einzugeben (siehe „Wiederkehrende Arbeitsabläufe“ auf Seite 9). Nach korrekter Eingabe der PIN erscheint die Nachricht.

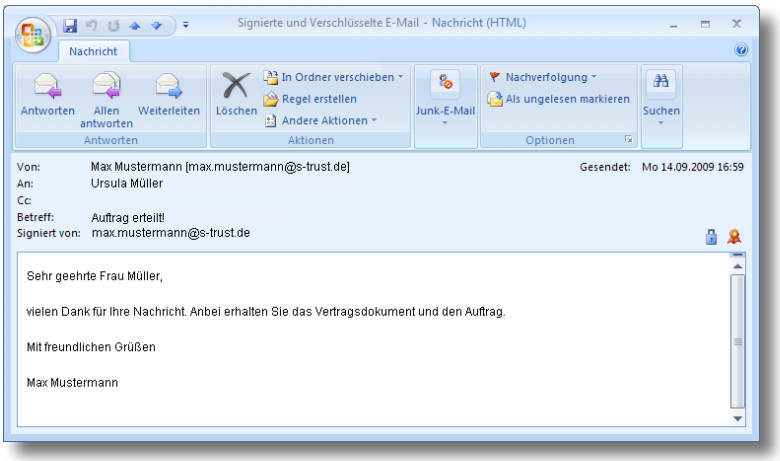

Abbildung 2.5: Outlook 2007 – verschlüsselte und signierte E-Mail

Bei einer signierten E-Mail wird am rechten Rand des E-Mail-Fensters das Symbol für signierte Nachrichten angezeigt, wurde die E-Mail verschlüsselt, wird das Symbol für verschlüsselte Nachrichten angezeigt. Ist die Nachricht sowohl signiert als auch verschlüsselt, erscheinen beide Symbole.

Informationen zur Signatur anzeigen
Informationen zur Signatur erhalten Sie bei Klick auf das Signatur-Symbol.

1. Klicken Sie auf das *Signatur-Symbol* am rechten Rand des E-Mail-Fensters. Es öffnet sich ein Fenster mit Informationen zur digitalen Signatur.

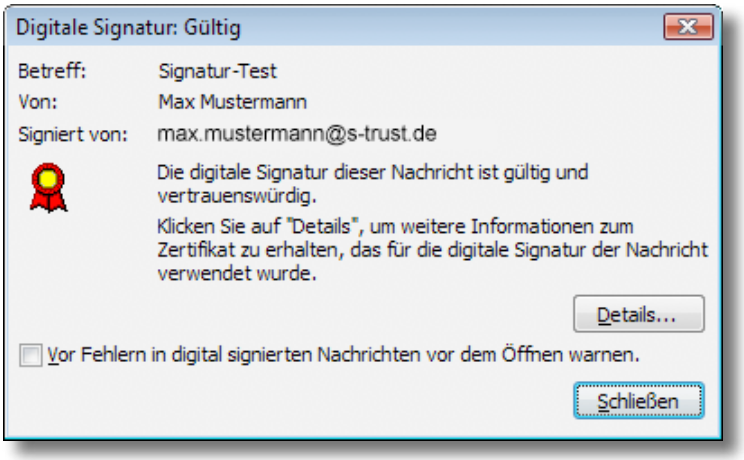
Digitale Signatur: Gültig
Betreff:
Signatur-Test
Von:
Max Mustermann
Signiert von:
max.mustermann@s-trust.de
Die digitale Signatur dieser Nachricht ist gültig und vertrauenswürdig.
Klicken Sie auf "Details", um weitere Informationen zum Zertifikat zu erhalten, das für die digitale Signatur der Nachricht verwendet wurde.
Details...
Vor Fehlern in digital signierten Nachrichten vor dem Öffnen warnen.
Schließen

Abbildung 2.6: Outlook 2007 – Informationen zur digitalen Signatur

Dieses Fenster enthält Informationen über die Vertrauenswürdigkeit der Signatur. Sollte der Inhalt der E-Mail nach dem Signieren verändert worden sein, wird dies hier angezeigt.

Über die Schaltfläche Details können Sie sich detaillierte Informationen zum verwendeten Zertifikat einblenden. Beachten Sie in diesem Zusammenhang auch die Informationen im Abschnitt „Gültigkeit eines Zertifikats“ auf Seite 8.

2. Schließen Sie das Fenster mit *Schließen*.

Informationen zur Verschlüsselung anzeigen
Informationen zur Verschlüsselung erhalten Sie ebenfalls auf Mausklick.

1. Klicken Sie auf das *Schloss-Symbol* am rechten Rand des E-Mail-Fensters. Es öffnet sich ein Informationsfenster, das den verwendeten Verschlüsselungsalgorithmus anzeigt.

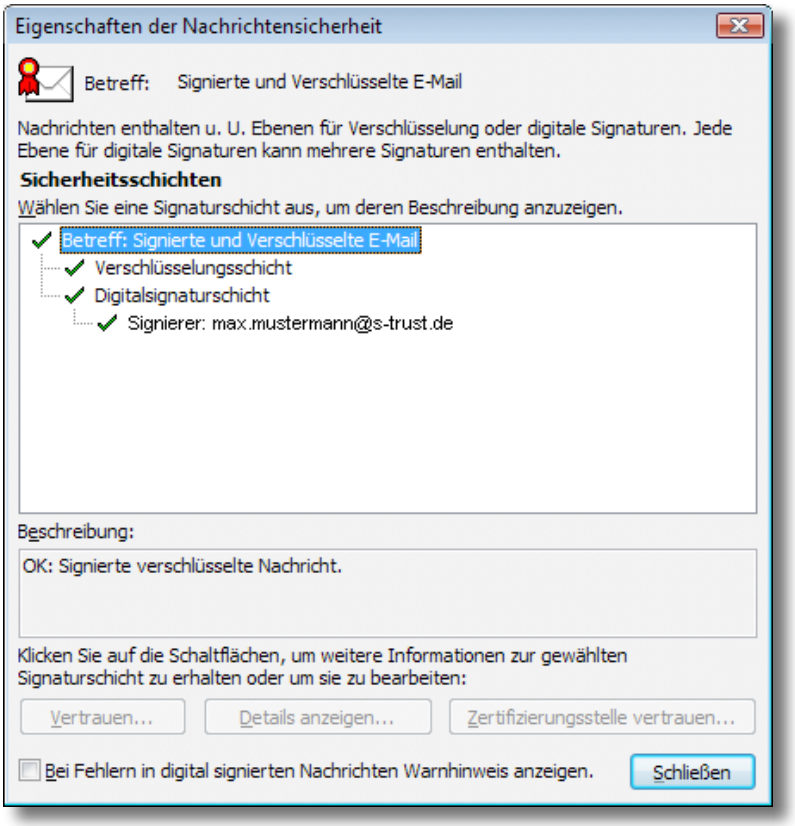
Eigenschaften der Nachrichtensicherheit
Betreff: Signierte und Verschlüsselte E-Mail
Nachrichten enthalten u. U. Ebenen für Verschlüsselung oder digitale Signaturen. Jede Ebene für digitale Signaturen kann mehrere Signaturen enthalten.
Sicherheitsschichten
Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen.
Betreff: Signierte und Verschlüsselte E-Mail
Verschlüsselungsschicht
Digitalsignaturschicht
Signierer: max.mustermann@s-trust.de
Beschreibung:
OK: Signierte verschlüsselte Nachricht.
Klicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten:
Vertrauen...
Details anzeigen...
Zertifizierungsstelle vertrauen...
Bei Fehlern in digital signierten Nachrichten Warnhinweis anzeigen.
Schließen

Abbildung 2.7: Outlook 2007 – Sicherheitsangaben zur verschlüsselten E-Mail

2. Klicken Sie auf den *Eintrag Signierer: name@server.de* und aktivieren Sie die Schaltfläche *Details anzeigen*. Es öffnet sich ein weiteres Fenster mit detaillierten Informationen zum verwendeten Zertifikat.

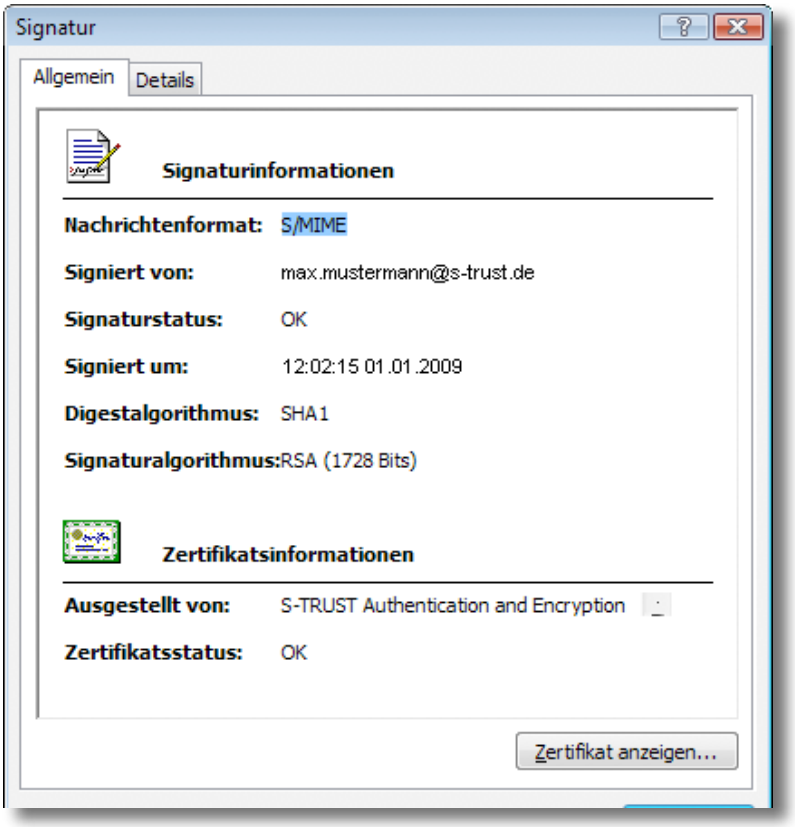

Abbildung 2.8: Outlook 2007 – Eigenschaften Signatur

3. Schließen Sie beide Fenster mit Schließen

Zertifikat des Absenders zum Adressbuch hinzufügen
Wenn Sie dem Absender künftig ebenfalls verschlüsselte Nachrichten senden möchten, speichern Sie den öffentlichen Schlüssel aus dem Zertifikat des Absenders in Outlook. Diesen Schlüssel haben Sie zusammen mit der signierten Nachricht vom Absender erhalten.

So speichern Sie das Zertifikat des Absenders im Adressbuch von Outlook 2007:

1. Klicken Sie in der E-Mail-Ansicht mit der rechten Maustaste auf den Absender der E-Mail.

2. Wählen Sie im Kontextmenü den Menüpunkt *Zu den Outlook-Kontakten hinzufügen*. Es öffnet sich ein Fenster mit einem neuen Adressbucheintrag.

3. Aktivieren Sie die Registerkarte *Zertifikate*.

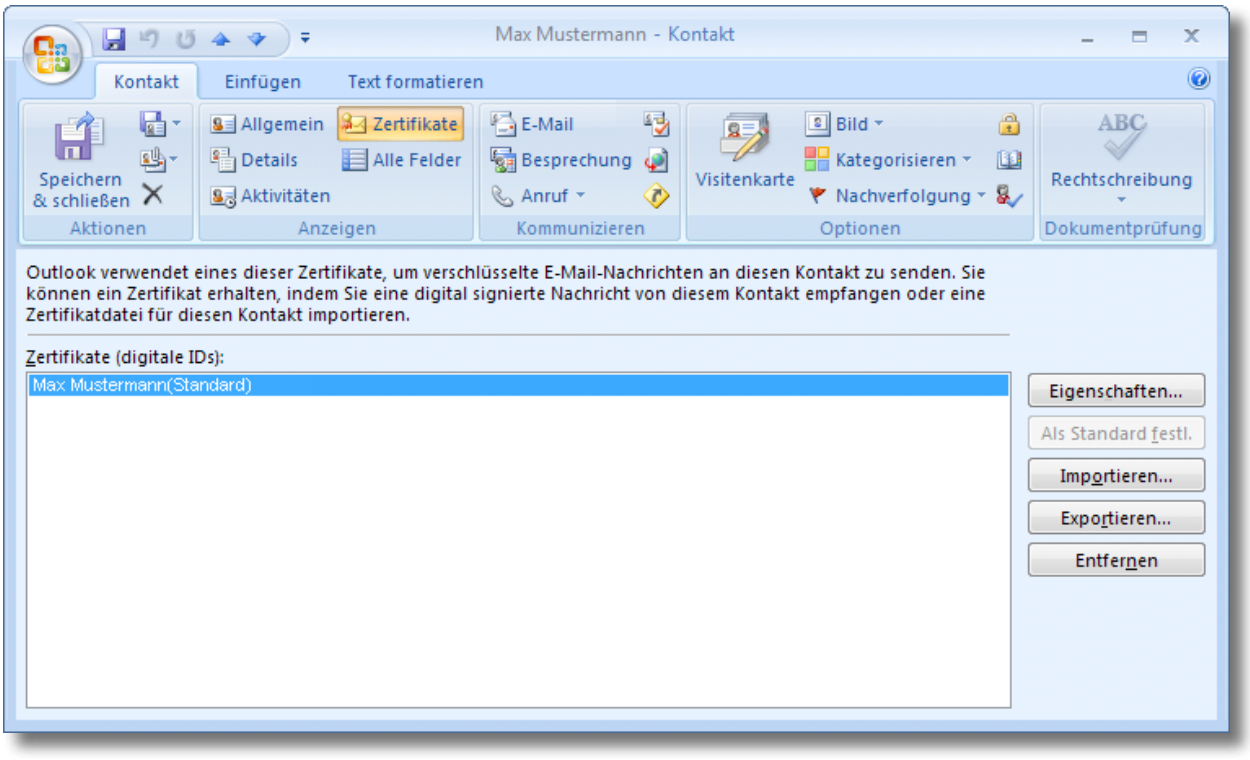

Abbildung 2.9: Outlook 2007 – Eintrag im Adressbuch

4. Klicken Sie auf die Schaltfläche *Eigenschaften*. Es öffnet sich das Fenster Zertifikatseigenschaften mit Informationen zum Zertifikat des Kontakts

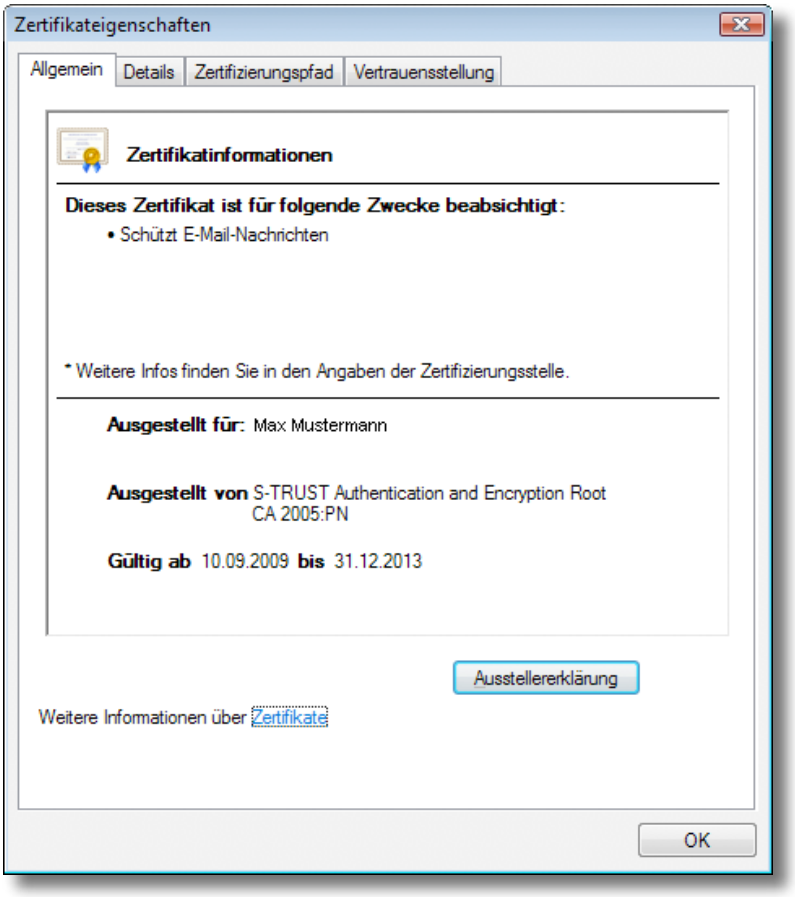

Abbildung 2.10: Outlook 2007 – Eigenschaften Signatur

5. Schließen Sie das Fenster Zertifikatseigenschaften mit *OK*. Sie befinden sich nun wieder im Fenster mit dem neuen Adressbucheintrag (Abb. 2.9).

6. Schließen Sie den Vorgang mit einem Klick auf die Schaltfläche *Speichern & Schließen* in der Symbolleiste unter Aktionen ab.

Mehrfach vorhandener Kontakt

Sollte der Absender bereits in Ihrem Adressbuch eingetragen sein, wird Outlook Ihnen beim Speichern des Zertifikats einen entsprechenden Hinweis geben (Abb. 2.11). In diesem Fall haben Sie die Wahl, einen neuen Kontakt mit diesen Daten anzulegen oder den vorhandenen Kontakt mit den Änderungen zu speichern.

Haben Sie von dem vorhandenen Kontakt zum ersten Mal ein Zertifikat erhalten, wählen Sie an dieser Stelle die Option **Vorhandenen Kontakt mit neuen Daten aus diesem aktualisieren**. Das Zertifikat ist damit im Adressbuch gespeichert.

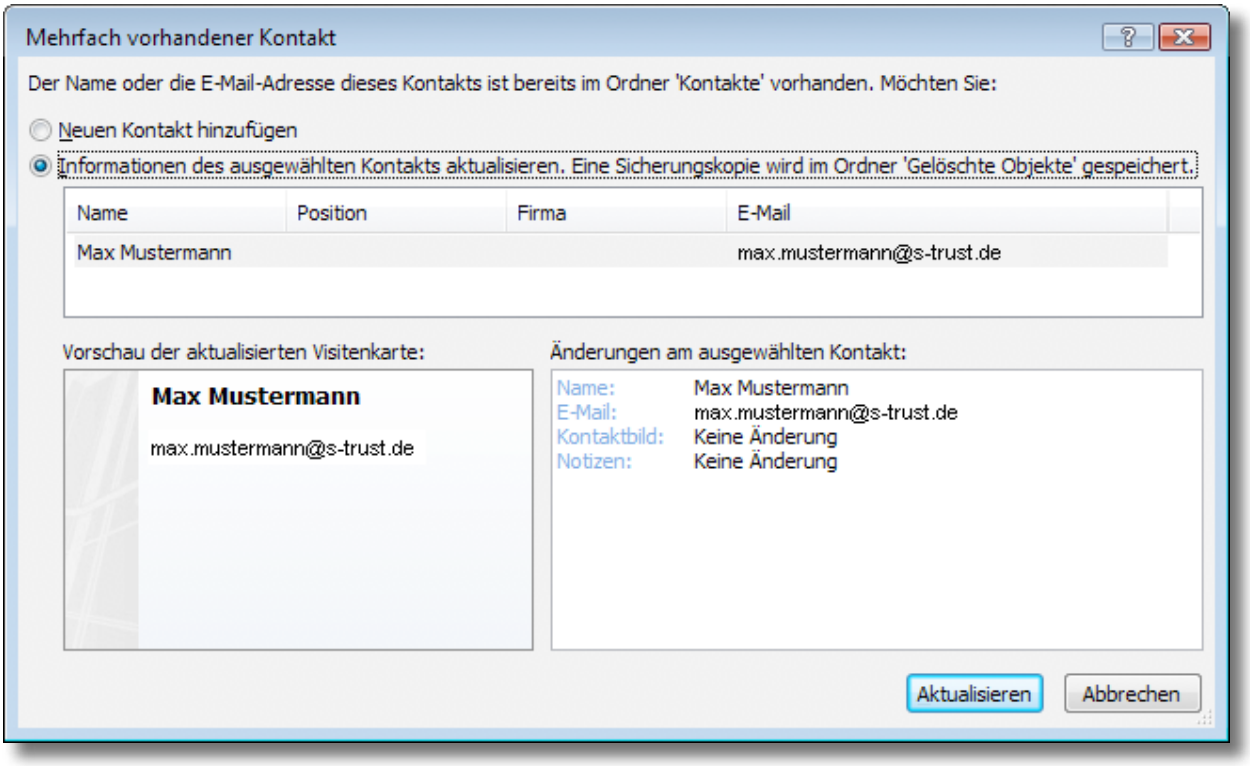

Abbildung 2.11: Outlook – Hinweis auf mehrfach vorhandenen Kontakt

3 Hinweise für Anwender anderer E-Mail-Programme

ACHTUNG:
Wenn Sie Ihre E-Mails mit einem Programm schreiben und verschlüsseln möchten, das nicht in den Benutzerhandbüchern beschrieben ist, beachten Sie bitte die Hinweise im Abschnitt „Unterstützte E-Mail-Programme“ auf Seite 5. Der Deutsche Sparkassenverlag übernimmt in diesem Fall keine Gewähr.
Nicht alle E-Mail-Programme unterstützen den Umgang mit Zertifikaten. Informieren Sie sich in der Dokumentation zu Ihrem E-Mail-Programm, ob es für die Verwendung von digitaler Signatur und Verschlüsselung nach dem S/MIME-Standard geeignet ist.

Anwender von Lotus Notes
Eine Kurzbeschreibung der wichtigsten Installationsschritte unter Lotus Notes finden Sie im Elektronischen Benutzerhandbuch von S-TRUST Sign-it.

Vorzunehmende Einstellungen
Bei der Einrichtung Ihres E-Mail-Programms sollten Sie, soweit in Ihrem Programm erforderlich und möglich, nachfolgend beschriebene Grundeinstellungen vornehmen. Achten Sie vor Beginn der Installation darauf, dass Ihr Kartenleser richtig installiert ist und sich Ihre signaturfähige Karte der Sparkassen-Finanzgruppe mit der elektronischen Signatur bereits im Kartenleser befindet.

1. **Installation des Kryptographie-Moduls**
   Rufen Sie in Ihrem E-Mail-Programm die Funktion zur Installation eines Kryptographie-Moduls auf und übergeben Sie dieser die folgende Datei: siqp11.dll.
   Sie finden die Datei im Installationsverzeichnis von S-TRUST Sign-it unter C:\Programme\S-TRUST Sign-it\ (Standardeinstellung).

2. **Installation der Wurzelzertifikate**
   Ihr Zertifikat wird nur als gültig anerkannt, wenn das Wurzelzertifikat (oder auch Root-Zertifikat) des Deutschen Sparkassenverlags auf Ihrem System installiert ist. Sie können zunächst prüfen, ob der Deutsche Sparkassenverlag unter Zertifizierungsstellen (Bezeichnung kann abweichen) bereits aufgeführt ist. Dann ist das Wurzelzertifikat bereits installiert. Andernfalls finden Sie die benötigten Dateien auf der Internetseite *www.s-trust.de* zum Download.

3. **Installation Ihres Zertifikats**
   Sie müssen in Ihrem E-Mailprogramm einstellen, mit welchem Zertifikat E-Mails signiert und verschlüsselt werden sollen. Aktivieren Sie dazu die entsprechende Funktion in Ihrem E-Mailprogramm. Bei der Auswahl wird Ihre Karte automatisch ausgelesen. Wählen Sie den Eintrag unter dem als Aussteller folgendes eingetragen ist: CN=S-TRUST Authentication and Encryption CA 200x:PN.

4. **Allgemeine Einstellungen**
   Wählen Sie in den Sicherheitseinstellungen Ihres Programmes die Verschlüsselungsstärke 168 Bits. Als Verschlüsselungsalgorithmus stellen Sie 3DES ein. Um Problemen beim Versand vorzubeugen, wählen Sie als Codierung bitte Unicode (UTF-8). Sie finden diese Einstellung in den Optionen meist unter Senden, Nachrichten Format oder E-Mails verfassen.

Spezifische Hilfe zu Ihrem E-Mail-Programm
Informationen zum genauen Vorgehen entnehmen Sie bitte der mit Ihrem E-Mail-Programm gelieferten Dokumentation und Online-Hilfe.

HINWEIS:
Falls Sie in der Dokumentation oder der Online-Hilfe zu Ihrem E-Mail Programm nach dem Stichwort „Signatur“ suchen, beachten Sie bitte, dass viele E-Mail-Programme mit dem Begriff „Signatur“ nicht nur die digitale Signatur bezeichnen. Damit können auch Fußzeilen gemeint sein, die das Programm automatisch am Ende einer Nachricht hinzufügt. Diese Signatur im Sinne einer Fußzeile enthält zum Beispiel oft eine Anschrift und hat nichts mit der digitalen Signatur im Sinne einer digitalen Unterschrift mithilfe eines Zertifikats zu tun.

4 Glossar

Codierung	Mit der Einstellung von Unicode (UTF-8) kann das E-Mail-Programm auch seltene Sonderzeichen korrekt verarbeiten. Das ist gerade bei elektronischen Signaturen elementar, da andernfalls die Signaturprüfung aufgrund unterschiedlicher Codierungen fehlschlägt.
CSA-PIN	PIN zur Verschlüsselung und Signatur von Daten oder E-Mails.
Digitale ID	Die digitale ID ist gewissermaßen die „Seriennummer“ eines Zertifikats. Damit ist eine eindeutige Zuordnung auch dann möglich, wenn ein Kontakt mehrere Zertifikate nutzt.
Digitale Signatur	Eine digitale Signatur (gesetzlich „Elektronische Signatur“) ist ein kryptografisches Verfahren, bei dem zu einer „Nachricht“ (d. h. zu beliebigen Daten) eine Zahl (die digitale Signatur) berechnet wird. Diese Signatur kann vom E-Mail-Programm geprüft werden. Damit ist sichergestellt, dass Dokumente von einem konkreten Absender verschickt und bei der Übertragung nicht verändert wurden. Mit digitalen Signaturen lassen sich sichere elektronische „Unterschriften“ erzeugen.
Elektronische Signatur s. auch Fortgeschrittene elektronische Signatur Qualifizierte elektronische Signatur	Die elektronische Signatur dient als „Unterschrift“ in elektronischer Form eines Dokuments oder einer E-Mail. Sie identifiziert zweifelsfrei den Absender. Der Inhalt eines unterzeichneten Dokuments kann nicht unbemerkt verändert werden.
Entschlüsselung	Als Entschlüsselung bezeichnet man die Umwandlung des Geheimtextes in den Klartext.
Fortgeschrittene elektronische Signatur s. auch Elektronische Signatur Qualifizierte elektronische Signatur	Fortgeschrittene elektronische Signaturen sind Signaturen, • die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, • die die Identifizierung des Signaturschlüssel-Inhabers ermöglichen, • die mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und • die mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt wird. Bei fortgeschrittener elektronischer Signatur wird das AE Zertifikat verwendet.

Kartenlesegerät	Für den Einsatz einer qualifizierten elektronischen Signatur wird mindestens ein Kartenlesegerät der Klasse 2 mit sicherer PIN-Eingabe benötigt.
Kryptografie	Kryptografie ist im ursprünglichen Sinne die Wissenschaft der Verschlüsselung von Informationen, die sich heute v. a. mit dem Schutz von Daten mittels mathematischer Verfahren beschäftigt.
MIME **s. auch S/MIME**	Multipurpose Internet Mail Extension. Mit diesem Standard wird Dokumenten ein bestimmtes, systemübergreifendes Format zugewiesen (Typisierung). Dadurch können Dokumente auf allen Systemen, die MIME-Typen unterstützen, korrekt verarbeitet werden.
PKCS-Schnittstelle	Diese Schnittstelle verbindet das E-Mail-Programm und das Kartenlesegerät und ermöglicht die Ver- und Entschlüsselung sowie das Generieren von digitalen Signaturen.
Qualifizierte elektronische Signaturen s. auch Elektronische Signatur Fortgeschrittene elektronische Signatur	Qualifizierte elektronische Signaturen sind elektronische Signaturen, die • auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und • mit einer sicheren Signaturerstellungseinheit erzeugt werden. Nur qualifizierte elektronische Signaturen sind in Deutschland gemäß §2 Nr. 3 Signaturgesetz (SigG) rechtswirksam, sie können in vielen Fällen die gesetzlich vorgeschriebene Schriftform ersetzen. Bei der qualifizierten elektronischen Signatur wird das qualifizierte Personenzertifikat verwendet.
S/MIME s. auch MIME	Ein Verfahren für den Austausch sicherer elektronischer E-Mails über das Internet, das von den meisten modernen E-Mail-Programmen unterstützt wird.
Sperrliste	siehe Zertifikatssperrliste
Verschlüsselung	Verfahren, um Daten und Dokumente sicher elektronisch zu übermitteln. Als Verschlüsselung bezeichnet man die Umwandlung eines Klartextes in Geheimtext, der nur mit einem passenden Schlüssel wieder entschlüsselt werden kann.
Verschlüsselungszertifikat	Zertifikat, das für den Verschlüsselungsvorgang eingesetzt wird.

Verzeichnisdienst	siehe Zertifikatsverzeichnis
Zertifikatssperrliste	In der Zertifikatssperrliste sind gesperrte Zertifikate aufgeführt. Bei Verlust, Diebstahl oder Kompromittierung der Sicherheit der Signaturkarte muss das Zertifikat gesperrt und damit für ungültig erklärt werden. Um sicherzugehen, dass bei der Zertifikatsprüfung kein gesperrtes Zertifikat akzeptiert wird, muss die Sperrliste in den Einstellungen von S-TRUST Sign-it regelmäßig aktualisiert werden.
Zertifikatsverzeichnis	Im Zertifikatsverzeichnis einer Zertifizierungsstelle werden alle durch sie ausgestellten Zertifikate aufgeführt. Diese können zur Prüfung einer Signatur oder zur Verschlüsselung einer Nachricht über das Internet heruntergeladen werden.
Zertifizierung	Bei der Zertifizierung eines öffentlichen Schlüssels wird die Zuordnung des Schlüssels zu einer Person durch die Zertifizierungsstelle beglaubigt. Die Identität der Person ist damit nachgewiesen.
Zertifizierungsstelle	auch Certification Authority (CA). Institution, die Personenzertifikate nach deutschem Signaturgesetz herausgibt und überprüft. Für die Ausgabe von fortgeschrittenen elektronischen Zertifikaten und qualifizierten elektronischen Signaturen müssen Zertifizierungsstellen strenge gesetzlichen Vorgaben erfüllen. S-TRUST ist eine solche Zertifizierungsstelle.

5 Index

A

Adressbuch
- Zertifikat hinzufügen 25

Allgemeine Informationen 3

B

Begriffserklärungen 29

C

CA s. Zertifizierungsstelle 31
Codierung 29
- einstellen (Outlook 2007) 18
- einstellen (Andere E-Mail-Programme) 28

CSA-PIN 29
- eingeben 10

D

Digitale ID 29
Digitale Signatur 29
Download
- Zertifikat 7

E

eingeben
- CSA-PIN 10

E-Mail-Adresse
- unterstützte 5

E-Mail-Programme
- unterstützte 5

empfangen
- signierte und verschlüsselte E-Mails 21

Entschlüsselung 29
entsperren
- Karte 11

erhalten
- Zertifikat des Empfängers 7

erstellen
- signierte und verschlüsselte E-Mails 22

erzeugen
- Signatur 9

F

Fachbegriffe 29
FAQ 3
fortgeschrittene Signatur 29

G

Glossar 29
Grundeinstellungen
- Outlook 2007 14

Grundlagen 3
Gültigkeit prüfen
- Zertifikat 8

H

häufig gestellte Fragen 3
Herausgeberzertifikat
- installieren 6

herunterladen
- Zertifikat 7

Hintergrundinformationen 3
Hotline 3

K

Kapitelübersicht 2
Karte
- entsperren 11

Kartenlesegerät 30
Kryptografie 30
Kryptografie-Modul 28

L

lesen
- signierte und verschlüsselte E-Mails 21

Lotus Notes
- Hinweise für Anwender 28

M

mehrere Zertifikate nutzen 4
MIME 30

Ö

öffentlicher Schlüssel 6
- erhalten 7
- integrieren 19

P

PIN
- eingeben 10

PIN-Eingabe 9
PKCS-Schnittstelle 30
privater Schlüssel 6
Programme
- unterstützte 5

Q

qualifizierte Signatur 30

S

S/MIME 30
Schlüssel
- erhalten 7
- öffentlich 6
- privat 6

schreiben
- signierte und verschlüsselte E-Mails 19

senden
- signierte und verschlüsselte E-Mails 20

Service Packs 5
sichere PIN-Eingabe 9
Sicherheitseinstellungen
- vornehmen 14

Signatur
- digitale 29
- elektronische 29
- erzeugen 9
- fortgeschrittene 29
- qualifizierte 30

Signieren
- als Voreinstellung 17

signierte E-Mail
- lesen 21
- schreiben 19

Sign-it 3
Softwarelizenz 4
Sperrliste 8
S-Trust Sign-it 3
- CSA-PIN eingeben 10
- Signatur erzeugen 9

Support 3
Systemvoraussetzung 4

T

technische Grundlagen 3
Telefonsupport 3
Testen 12
Testlizenz 4

U

unterstützte E-Mail-Programme 5
Updates 5

V

Verschlüsselung 30
- als Voreinstellung 17

verschlüsselte E-Mail
- lesen 21
- schreiben 19

Verschlüsselungsalgorithmus
- einstellen (andere E-Mail-Programme) 28
- einstellen (Outlook 2007) 15

Verschlüsselungsstärke
- einstellen (andere E-Mail-Programme) 28
- einstellen (Outlook 2007) 15

Verschlüsselungszertifikat 30
Verzeichnisdienst 31
Voreinstellung
- Signieren und Verschlüsseln 17

Z

Zertifikat
- erhalten 7
- Gültigkeit prüfen 8
- herunterladen 7
- zum Adressbuch hinzufügen 25

Zertifikate
- auswählen (andere E-Mail-Programme) 28
- auswählen (Outlook 2007) 16
- installieren (andere E-Mail-Programme) 28

Zertifikatssperrliste 31
Zertifikatsverzeichnis 31
Zertifizierung 31
Zertifizierungsstelle 31

Impressum

Deutscher Sparkassen Verlag GmbH
Postanschrift: 70547 Stuttgart
Hausanschrift: Am Wallgraben 115, 70565 Stuttgart
Telefon: +49 711 782-0
Telefax: +49 711 782-1635
E-Mail: info@s-trust.de

Aufsichtsratvorsitzender: Dr. Siegfried Naser, Sitz der Gesellschaft: Stuttgart, Registergericht: Stuttgart, Handelsregister: Nr. B/748, Bankverbindung: Baden-Württembergische Bank (BW-Bank), BLZ: 600 501 01, Konto: 1366860, USt. ID-Nr.: DE 147830796, Geschäftsführung: Dr. Bernd Kobarg (Vorsitzender), Wilhelm Gans, Oliver Lux, Jürgen Schneider
© 2009 Deutscher Sparkassen Verlag GmbH, Stuttgart
Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

So viel Lösung,
wie sie brauchen.

E-Mails signieren und verschlüsseln

S-TRUST
Deutscher Sparkassen Verlag GmbH
Am Wallgraben 115
70565 Stuttgart
info@s-trust.de
www.s-trust.de

DSV*Gruppe*

Deutscher Sparkassenverlag
AM | COMMUNICATIONS
Deutsche Sparkassen Datendienste
EPC Electronic Payment Cards
S-CARD Service
B+S Card Service
DSV Logistik
SEG Sparkassen-Einkaufsgesellschaft
MehrWert Servicegesellschaft